ABSTRACT OF THE DISCLOSURE

A SYSTEM AND METHOD FOR CRYPTO-KEY GENERATION AND USE IN CRYPTOSYSTEM

A first processor generates a private crypto-key and a public crypto-key. The first processor divides the private crypto-key into two portions, a first private key portion, based upon a user's password, and a second private key portion. The private crypto-key and the first private key portion are then destroyed. The remaining portion, second private key portion, and the public crypto-key are stored in a memory. A second processor generates the first private key portion based upon the user's password and responsive to receiving the user's password. The second processor then destroys the generated first private key portion with out storing the generated first private key portion.